Testimony

STATEMENT OF
ROBERT J. LIEBERMAN
DEPUTY INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY,
VETERANS AFFAIRS AND INTERNATIONAL RELATIONS,
HOUSE COMMITTEE ON GOVERNMENT REFORM
ON
TOP DEFENSE MANAGEMENT CHALLENGES

Report No. D-2001-083 DELIVERED: March 15, 2001

Office of the Inspector General
Department of Defense

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 15Mar01	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Statement of Robert J. Lieberman Deputy Inspector General Department of Defense Before the Subcommittee on National Security, Veterans Affairs and International Relations, House Committee on Government Reform on Top Defense Management Challenges	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Number(s)** D-2001-083
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
I am pleased to be here this morning to discuss the management challenges facing the Department of Defense, from the standpoint of its internal auditors and investigators. My testimony will summarize and update the written analysis that we provided to various congressional leaders last December 1. * In that analysis, we identified 10 areas, each containing multiple significant challenges. Those areas were: (1) information technology management, especially acquiring new systems; (2) information system security; (3) other security concerns; (4) financial management; (5) acquisition of weapons, supplies and services; (6) peacetime health care; (7) supply inventory management; (8) other infrastructure issues; (9) readiness; and (10) human capital management.

Subject Terms

Document Classification unclassified	**Classification of SF298** unclassified

Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 25	

Mr. Chairman and Members of the Committee:

I am pleased to be here this morning to discuss the management challenges facing the Department of Defense, from the standpoint of its internal auditors and investigators. My testimony will summarize and update the written analysis that we provided to various congressional leaders last December 1.* In that analysis, we identified 10 areas, each containing multiple significant challenges. Those areas were: (1) information technology management, especially acquiring new systems; (2) information system security; (3) other security concerns; (4) financial management; (5) acquisition of weapons, supplies and services; (6) peacetime health care; (7) supply inventory management; (8) other infrastructure issues; (9) readiness; and (10) human capital management.

Information Technology Management

Information systems are now as crucial to DoD management activities as the central nervous system is to the human body. Managers at all levels, regardless of their functions, depend on information that is compiled, analyzed, adjusted and reported with automated systems. During the Year 2000 computer conversion project, approximately 10,000 DoD computer networks were inventoried and the true extent of the Department's dependence on those systems became well understood for the first time. The magnitude of DoD spending on information technology is less well identified, but clearly it far exceeds $20 billion annually.

Given the considerable dependence on "IT" and the high cost of large system investments, the historically poor record of the DoD for controlling the proliferation of incompatible systems with nonstandard data elements, acquiring new systems that meet user needs within reasonable timeframes, controlling cost, and ensuring the quality and security of data has been a major concern. Recognizing that such problems are common across the Federal Government, the Congress specified in the Clinger-Cohen Act of 1996 that Chief Information Officers in each agency would oversee well disciplined information technology acquisition processes. This is a daunting challenge for a department with 71 major information system acquisition projects and hundreds of "smaller" system acquisition and modification projects belonging to dozens of organizations. The DoD has been candid about the need for more effective management controls in this crucial

* The letters of December 1, 2000 and the last several Inspector General Semiannual Reports to the Congress, which contain similar analyses of high risk areas, are available on-line at www.dodig.osd.mil.

area, but progress has been slow and the goals of the Clinger-Cohen Act have not yet been achieved.

I have mentioned the challenge of information system investments first because poor information is at the root of a very large number of DoD management problems, ranging from difficulty in making cost comparisons to poor supply inventory management practices. Due to your series of hearings on the backlog of personnel security clearance investigations, I know that you are particularly well aware of the serious problems caused by the failure of the Defense Security Service's Case Control Management System. Its problems were particularly egregious, but not unique by any means.

The Department has revised its basic information system acquisition procedures and tried to be responsive to our recommendations. Nevertheless, we believe this area deserves continued close attention as DoD experiments with portfolio management, integrated product teams and other management oversight concepts. At the present time, virtually every information technology project that we audit exhibits significant management problems. Those flaws include poorly defined requirements and frequent user dissatisfaction.

Information System Security

Another facet of information technology management is assuring the security of DoD systems and information. Guarding against the interception of military signals is an age-old problem and, until recently, was chiefly the province of the cryptographers. Although the DoD must always maintain tight security for its classified systems, the past few years have seen the massive expansion of networked and unclassified DoD information systems. In turn, this expanded DoD presence on the Internet has led to a proliferation of attacks and intrusions.

Unauthorized access to computer networks poses a multifaceted threat to national security that cuts across society's boundaries: it potentially affects both the public and private sectors, transcends national borders, and can cause problems in virtually all economic sectors and levels of government. To organizations, the threat is both internal and external, and constantly evolving. Perpetrators can include disgruntled or irresponsible employees, criminals, hobbyist hackers, agents of hostile states and terrorists.

Recent audits indicate that much more needs to be done to implement the Defense Information Assurance Program fully and to sustain a robust effort indefinitely, as 21st Century realities will demand. Although it was widely assumed that the successful management approaches and mechanisms developed to overcome the "Y2K" problem would be readily transferable to the information assurance challenge, this has occurred to a very limited extent.

The strongest part of the DoD effort currently is in the areas of intrusion detection and incident response. Several Defense Criminal Investigative Service agents, from my office, are an integral component of the Joint Task Force on Computer Network Defense, which gives DoD a powerful capability and is an excellent example of cooperation between the DoD information security and Federal law enforcement communities.

Consistent policies, procedures, training and security assessments in DoD computing centers and among system users remain weaker areas. In that regard, the Government Information Security Reform provisions of the National Defense Authorization Act for Fiscal Year 2001, which mandate annual information assurance assessments and IG validation audits in Federal agencies, should be very helpful in terms of focusing management attention on this problem area. It does not appear that DoD has done sufficient planning at this point to be able to conduct a comprehensive self-assessment this year. Nevertheless, one would expect to see significant incremental improvement each year and I recommend that Congress extend these reporting requirements beyond their current sunset date of October 30, 2002.

Other Security Concerns

In addition to the threat posed by unauthorized intrusion into DoD information systems, a wide range of other security issues confront the DoD. Those threats include terrorism against U.S. personnel and facilities, conducted by either conventional or non-conventional means, and the disclosure or theft of sensitive military technology. The terrorist attack on the USS COLE in Yemen and security breaches at the FBI, the Department of Energy, the Central Intelligence Agency and DoD graphically demonstrated that security vulnerabilities need to be matters of utmost concern.

Recent audits have indicated that the DoD needs to improve security measures to guard against both internal and external threats. We have not audited force protection issues, but we

have extensively reviewed a number of other areas where unacceptable vulnerability exists. These include, as previously mentioned, the Defense Personnel Security Program, whose capability to handle the investigative workload basically collapsed in the late 1990's.

Similarly, there is a consensus in the Executive Branch and Congress that the export license regime of the 1990's was inefficient and probably ineffective in controlling the unintended loss of U.S. military technology. During 2000, the DoD worked with other Federal agencies to streamline the licensing processes and approved additional resources to improve the speed and value of license application reviews. The task of determining to what extent the fundamental national export control policies need to change, however, remains unfinished business for the new Administration and Congress.

Recent audits have indicated that issues such as properly demilitarizing military equipment before disposal and controlling the access of contractors and visitors to technical information at military engineering organizations and laboratories need more attention.

Financial Management

The DoD made several major financial management improvements during the 1990's, but needs further reform and more senior management attention to address a wide range of serious concerns.

Perhaps the best known of those problems is that the DoD remains unable to comply with the requirements in the Chief Financial Officers Act of 1990 and related legislation for auditable annual financial statements. The results of audits of the DoD-wide and other major financial statements for FY 2000 were essentially the same as in previous years. The Military Retirement Fund statements received a clean audit opinion, but all other major DoD financial statements were unauditable. Previous goals for obtaining clean opinions on all or most annual year-end statements during the FY 2000 timeframe were unrealistic and it is unclear what a realistic goal would be at this point. A couple of relatively small DoD organizations and funds have achieved favorable opinions or may do so in the near future, but I see little prospect for a clean opinion on the DoD-wide year-end financial statements before the middle of this decade.

The root problem is that DOD lacks modern, integrated information systems that can compile auditable year-end financial statements. This also means that the financial data provided daily, weekly or monthly to managers and commanders is often unreliable.

During the past year, the DoD made hopeful progress in addressing major impediments to favorable audit opinions. These problems cannot be solved quickly and some could not be addressed previously until new Federal accounting standards were issued and interpreted, which is still an incomplete process and is not controlled by DoD. Policies were issued to implement several new accounting standards and more contractors were engaged to provide their expertise on a variety of issues, such as determining the value of different categories of property.

Most importantly, the Department took steps to apply the lessons learned from the successful DoD Y2K conversion program to the financial system compliance effort. The DoD Senior Financial Management Council, which had not met for several years, was reconstituted to ensure senior management control. A comprehensive program management plan was issued on January 5, 2001.

We strongly recommended this initiative. Indeed, I believe it is the most heartening development in this area in several years. I urge the new Administration and Congress to support this adaptation of the successful Y2K management approach to the somewhat similar information systems challenge involved in attaining CFO Act compliance. The Defense Financial Management Improvement Plan shows cost estimates of $3.7 billion for FY 2000 through FY 2003 to make critical reporting systems compliant with applicable standards. We believe those estimates are understated. With proposed spending of that magnitude, it is imperative that a highly disciplined management approach be used.

The new approach will fill a long-standing gap by providing good performance measures for the most important aspect of the DoD financial management improvement effort. As welcome as those metrics will be for measuring system compliance status, however, even they will not measure the usefulness of the data to managers, appropriators or budget committees. Numerous recent statements and testimony to Congress by the Office of Management and Budget, GAO and DoD officials have stressed that the ultimate goal of financial management reform legislation is ensuring useful financial information for sound decision-making

by managers throughout the year, not merely audit opinions on year-end financial statements. We agree. Audit opinions are a simple and readily understandable metric, but judging the usefulness of financial information is far more difficult. Likewise, audit opinions on financial statements provide little insight into the efficiency of functions such as paying contractors or capturing the cost of operations of individual bases and work units. The DoD has long-standing deficiencies in both of those areas.

Finally, we believe that the seemingly never-ending growth of complexity in the DoD chart of accounts needs to be reversed. It is incongruous that credit card companies can manage millions of accounts with 16 digits but DoD needs to put lines of accounting with up to more than 200 digits on huge numbers of contracts, vouchers and other documents, making frequent errors unavoidable. The system is designed to protect the integrity of hundreds of thousands of accounts as hundreds of millions of transactions are made, but accuracy is impossible and meanwhile many managers find the official accounting records to be of little use for day to day decision-making.

Acquisition

The DoD is working toward the goal of becoming a world-class buyer of best value goods and services from a globally competitive industrial base. The Department hopes to achieve this transformation through rapid insertion of commercial practices and technology, business process improvement, creating a workforce that is continuously retrained to operate in new environments, and heavily emphasizing faster delivery of material and services to users. In order to fulfill these objectives, the DoD has initiated an unprecedented number of major improvement efforts, including at least 40 significant acquisition reform initiatives.

Despite some successes and continued promises from ongoing reforms, the business of creating and sustaining the world's most powerful military force remains expensive and vulnerable to fraud, waste and mismanagement. In FY 2000, the DoD bought about $156 billion in goods and services, with 15 million purchasing actions. The Department currently is attempting to stretch its acquisition budgets across 71 major programs, estimated to cost $782 billion, and 1,223 smaller programs worth $632 billion.

The scope, complexity, variety and frequent instability of Defense acquisition programs pose particularly daunting management challenges. Aggressive acquisition cost reduction goals have been established, but it is too soon to tell if they are achievable. Many specific initiatives have not yet been fully implemented and are in a developmental or pilot demonstration phase.

In the push to streamline procedures and incorporate commercial practices and products, the Department cannot compromise its insistence on quality products and services at fair and reasonable prices. An inherent challenge throughout the Department's acquisition reform effort is ensuring that critically needed controls remain in place and there is proper oversight and feedback on new processes. Recent audits continued to indicate a lack of effective means for identifying best commercial practices and adapting them to the public sector; overpricing of spare parts; inattention to good business practices and regulations when purchasing services; poor oversight of the several hundred medium and small acquisition programs; and adverse consequences from cutting the acquisition workforce in half without a proportional decrease in workload.

Although the DoD must continue to address the challenges of how to control the cost of purchased goods and services, the most fundamental acquisition issues confronting the Department relate to requirements and funding. The expanding national dialogue on military missions and the ongoing Defense Review may result in radical changes to DOD missions, military force structure and acquisition requirements. Whether changes in requirements and the topline budget ultimately are major or relatively minor, there needs to be a far-reaching rebalancing of acquisition programs to match available funding.

Finally, we believe that the Department needs to put more acquisition reform emphasis on ensuring the quality, serviceability and safety of purchased equipment, parts and supplies. Concentrating on prices and timely delivery is vital, but quality should be the most important attribute for DoD purchases, especially for materiel used by the warfighters. Minimizing vulnerability to fraud, especially false statements regarding product testing and product substitution, remains imperative. We currently have nearly 700 open procurement fraud investigations and there were 134 convictions, with recoveries of $170 million, from procurement fraud cases during FY 2000.

Health Care

The Military Health System (MHS) costs over $20 billion annually and serves approximately 8.2 million eligible beneficiaries through its health care delivery program TRICARE. TRICARE provides health care through a combination of direct care at Military Department hospitals and clinics and purchased care through managed care support contracts. The MHS has dual missions to support wartime deployments (readiness) and provide health care during peacetime. The MHS faces multiple challenges: attaining full funding, cost containment, transitioning to managed care, and data integrity.

Cost containment for peacetime health care is challenged by program expansion, historically poor budget estimating techniques, lack of good cost information and significant levels of health care fraud. Lack of comprehensive patient-level cost data has made decisions on whether to purchase health care or provide the care at the military treatment facility more difficult.

To combat health care fraud, the Defense Criminal Investigative Service has developed an active partnership with the TRICARE Management Activity to give high priority to health care fraud cases, which comprise a growing portion of the overall investigative workload. We have about 500 open criminal cases in this area. In FY 2000, our investigations led to 94 convictions and $529 million in recoveries.

Supply Inventory Management

Supply management to support U.S. military forces, which are located around the world and use several million different types of weapon systems, other equipment, spare parts, fuel, apparel, food items, pharmaceuticals and other supplies, may be the most difficult logistics challenge in the world. Despite the clear need to modernize DoD supply operations, it should be noted that U.S. military logistics performance has been excellent in demanding situations such as recent deployments to comparatively remote areas of the world.

Every facet of supply management involves challenges and it is critically important to recognize that weapon systems and other equipment must be designed, selected and procured with logistics support as a paramount concern. The use of standardized parts, commercial items, non-hazardous materials and easy to maintain components will considerably ease the supply support problem for

each system or piece of equipment. Conversely, inattention to such factors during acquisition will increase the risk of higher costs and logistics failures.

The logistics community relies heavily on program managers and operators to help forecast supply requirements, and historically this has been very difficult. The Department has been justifiably criticized for accumulating excessive supply inventories, but supply shortfalls are at least as great a concern due to the impact on readiness. Current logistics reform initiatives are principally focused on introducing private sector logistics support practices, which in turn are based on applied web-based technology. The DoD has initiated a myriad of logistics improvement initiatives, most of which are still in early stages. For example, the Defense Logistics Agency started a five year "logistics makeover" of its acquisition, processing and distribution practices last August. As logistics reform continues, we anticipate continuing valid concerns about all phases of supply support, including requirements determination, procurement, distribution, and disposal.

Other Infrastructure Issues

Despite numerous management initiatives to reduce support costs so that more funds could be applied to recapitalizing and ensuring the readiness of military forces, more can and should be done. Organizations throughout the Department need to continue reengineering their business processes and striving for greater administrative efficiency.

Unfortunately, cutting support costs can easily become counterproductive if the quality of support services and facilities is degraded. In addition, there are numerous bona fide requirements in the support area that will be expensive to address. For example, the average age of structures on military installations is 41 years and wholesale recapitalization is needed. In the category of family housing alone, a third of the 285,000 units require replacement in the next several years. The backlog of real property maintenance is $27.2 billion.

The area with the most promise for reducing installation level costs is base closures. Some DoD studies indicate that the base facility infrastructure exceeds requirements by 23 percent. We believe one or possibly two more rounds of base closure and realignment would be prudent national policy.

Readiness

Concern about the readiness of U.S. military forces was a principal issue last year in congressional hearings and was addressed during the Presidential election campaign. There is a fairly broad consensus that readiness shortfalls exist, although the extent of impairment to mission capability is more contentious. Clearly, there are spare parts shortages; significant backlogs for depot maintenance ($1.2 billion); concerns related to recruiting, retention and morale; disproportionately numerous deployments for some units; unanticipatedly high operating tempo; and equipment availability problems. In response, the DoD and Congress have made major budget adjustments and military entitlements have been expanded. The Department's readiness posture ultimately depends, however, on the effectiveness of hundreds of support programs, which range from training to supply management.

The DoD audit community supported the successful program to overcome the Year 2000 computer challenge, which the Department considered to be a major readiness issue, with the largest audit effort in DoD history. The IG, DoD, issued 185 "Y2K" reports. Due to that massive commitment, resource constraints and other workload, our recent coverage of other readiness issues was severely limited. We plan to restore at least some of the necessary coverage during FY 2001, continuing our particular concentration on chemical and biological defense matters. On January 31, for example, we issued a report on the establishment of National Guard Weapons of Mass Destruction-Civil Support Teams. The audit indicated they were not yet ready for certification as mission-ready. We are working with the involved DoD organizations to ensure that the concerns related to those certifications are expeditiously and fully addressed. Likewise, we are reviewing the accuracy and usefulness of a number of performance measurements reported by DoD to the Congress, many of which relate to readiness.

Human Capital

Like most government organizations, DoD faces a range of serious personnel management issues. The deep cuts in both the military force structure and the civilian workforce after the end of the Cold War were not accompanied by proportionate reductions in military force deployments or in civilian workload. On the contrary, military operations tempo has been very high and there have been indications of morale problems among both military and civilian personnel. Among the negative effects of downsizing

are increased retention problems because of slow promotions and overworked staffs, recruiting problems and skills imbalances.

Human capital concerns apply in virtually all segments of the workforce. Our February 2000 report on the impact of cutting the DoD acquisition workforce in half was received with considerable interest by both the DoD and Congress. The Federal Chief Information Officers Council has been pushing vigorously for attention to problems in the information technology workforce. The Military Department Surgeons General have testified to Congress on the detrimental effect of cutting medical staff by 30 percent, without proportionate decreases in military treatment facility workload. The Secretary of Defense Annual Report to the President and the Congress for 2001 includes the following analysis of the DoD Test and Evaluation (T&E) community:

"Since 1990, the T&E business area has reduced government personnel by more than 40 percent, and T&E institutional budgets by 30 percent. Over this same period, developmental test and evaluation workload has remained essentially stable, and operational test and evaluation workload has significantly increased. As a result, T&E is not sufficiently funded or manned to effectively and efficiently address the test and evaluation challenges of the next decade. To be responsive to the philosophy of early use of T&E for discovery of military effectiveness and suitability issues, T&E personnel will be overextended. While the principles of the faster, better, cheaper acquisition reform philosophy are sound, the implementation which has stretched the resources of T&E has also resulted in a rush-to-failure mode for some acquisition programs."

In addition to rethinking what workforce size is needed to meet mission requirements, as opposed to cutting mission capability to meet arbitrary personnel reduction goals, the DoD needs to develop more effective training methods to enable continuous learning to keep abreast of emerging technology and changing management practices. It also must find ways to compensate for the pending retirement of a large portion of the experienced workforce, improve competitiveness with private industry, and develop better incentives for productivity improvement.

The recent initiatives on improving military pay and benefits, the development of a pilot personnel management reform program for acquisition personnel, and other new initiatives indicate

that human capital issues are now in the forefront of management concerns.

Summary

This has been a broad brush treatment of a large and complicated picture. A list of some of the FY 2001 audit reports pertaining to the top ten problem areas is attached for further information. In closing, I would like to emphasize that, on the whole, DoD managers react positively and generally do their best to correct the problems identified by my office. The Department agreed to take responsive action on 96 percent of the over 3,000 recommendations made in Inspector General, DoD, reports during the past three years. The fact that serious problems persist is generally attributable to their inherent difficulty or to conflicting priorities, rather than indifference toward the best interest of the Department and the taxpayer, and at least some progress is evident in all areas. The prospect of the new administration bringing fresh viewpoints and insights to bear on these problems also bodes well for making more progress on them.

This concludes my written statement.

Attachment

SELECTED INSPECTOR GENERAL, DEPARTMENT OF DEFENSE REPORTS FROM FY 2001

INFORMATION TECHNOLOGY MANAGMENT

D-2001-019 Program Management of the Defense Security Service Case Control Management System, December 15, 2000

The Defense Security Service did not effectively manage the high risk involved in the integration of the Case Control Management System and the Enterprise System. As a result, those systems had significant limitations and were insufficiently tested and evaluated for operational effectiveness prior to deployment in October 1998, leading to failures that degraded Defense Security Service productivity. As of September 2000, project management had been greatly improved, but high risks remained. Resolution of design problems was continuing and measurements for reliability and maintainability at production objectives were still needed.

The Air Force Program Management Office had developed a phased acquisition strategy to stabilize the Case Control Management System and the Enterprise System with product improvements and incrementally migrate it to an improved Enterprise System architecture between FY 2002 through FY 2008. However, the DoD needs to consider alternative solutions for processing personnel security investigations before further decisions are made on future system architecture.

D-2001-030, Oversight of Defense Finance and Accounting Service Corporate Database, December 28, 2000

There was high risk that DoD would not be able to achieve its goal of a single, integrated system, because management was focused on individual systems and system ownership is fragmented among many DoD Components. A more integrated management approach is needed to attain the full benefits associated with initiatives such as the Defense Procurement Payment System, Defense Standard Disbursing System, Defense Cash Accountability System, and Defense Departmental Reporting System. These benefits are a standard system for the business areas and a single database to store information.

D-2001-015, Defense Environmental Security Corporate Information Management (DESCIM) Program, December 7, 2000

The DoD did not effectively implement and manage the DESCIM Program, which did not achieve its stated goal of developing a standard system to meet mission reporting and management information requirements. The DoD spent 9 years and $100 million on DESCIM.

D-2001-014, Development and Implementation of a Joint Ammunition System, December 6, 2000

The DoD spent 8 years and $41.3 million developing a new system for the logistical and financial reporting of the ammunition inventory. Despite those efforts, DoD did not produce a working system. During the audit, DoD suspended work on the most recent development effort, the Joint Ammunition Management Standard System, and began considering other alternatives. However, DoD personnel were not adequately considering an existing Navy system, the Conventional Ammunition Integrated Management System, as one of the alternatives. Navy personnel indicated that, with limited modification, the Conventional Ammunition Integrated Management System would be capable of meeting mission requirements. Otherwise, DoD would spend $71 million unnecessarily and be forced to use multiple non-compliant systems in the meantime.

INFORMATION SECURITY

D-2001-046, Information Assurance at Central Design Activities, February 7, 2001

The three Central Design Activities we visited had not certified or accredited their software development environments as required by DoD policy. In addition, those Central Design Activities did not participate in the accreditation of software development environments created for them and housed at Defense Information Systems Agency facilities. As a result, there is an increased risk of unauthorized access to and modification of DoD software. Likewise, controls were inadequate to detect and remove malicious code from some software products under development at these sites.

D-2001-029, General Controls Over the Electronic Document Access System, December 27, 2000

System security controls were insufficient and additional efforts to improve security by several DoD organizations were needed.

D-2001-013, DoD Compliance With the Information Assurance Vulnerability Alert Policy, December 1, 2000

The Deputy Secretary of Defense issued an Information Assurance Vulnerability Alert (IAVA) policy memorandum on December 30, 1999. Recent events demonstrated that widely known vulnerabilities exist throughout DoD networks, with the potential to severely degrade mission performance. The policy memorandum instructs the Defense Information Systems Agency to develop and maintain an IAVA database system that would ensure a positive control mechanism for system administrators to receive, acknowledge, and comply with system vulnerability alert notifications. The policy requires the Commanders in Chief, Services, and Defense agencies to register and report their acknowledgement of and compliance with the IAVA database. According to the policy memorandum, the compliance data to be reported should include the number of assets affected, the number of assets in compliance, and the number of assets with waivers. The policy memorandum provided for a compliance review by the Inspector General, DoD.

As of August 2000, DoD progress in complying with the policy memorandum had not been consistent. At that time, all 9 Commanders in Chief, 4 Services, and 14 Defense agencies had registered as reporting entities with the IAVA database, but 4 other DoD Components had not. Also, information contained in the database for the alerts posted in 2000 showed that of the Components that had registered, only four Commanders in Chief, one Service, four Defense agencies, and two other DoD Components had reported compliance in accordance with the IAVA policy. As of November 2000, however, DoD had made significant progress.

D-2001-017, Unclassified but Sensitive Internet Protocol Router Network Security Policy, December 12, 2000

The DoD lacked authoritative and current policy to ban unauthorized Internet access connections. As a result, individual installations and commands may have made questionable decisions on commercial Internet access, complicating the security challenge.

D-2001-016, Security Controls Over Contractor Support for Year 2000 Renovation, December 12, 2000

The DoD Components used techniques, such as access controls, configuration management, and code verification, to monitor and control contractor access to the 159 mission-critical systems in

our sample that were renovated by contractor personnel during the year 2000 renovation effort. However, they did not assess risk for 103 of those 159 systems and did not reaccredit 119 systems from a security standpoint. As a result, at least seven DoD Components were not assured that documented security postures were valid. Further, potential risks to the mission-critical systems were unknown and the systems may be exposed to increased risk of unauthorized access and modification.

OTHER SECURITY CONCERNS

D-2001-065, DoD Adjudication of Contractor Security Clearances Granted by the Defense Security Service, February 28, 2001

Defense Security Service case analysts, in granting security clearances to DoD contractors, were using processes that did not meet the requirements of Executive Order 12968, "Access to Classified Information," August 4, 1995, which requires appropriately trained adjudicators and uniform standards for granting security clearances. As a result, contractor clearances may not have been properly justified in all instances.

D-2001-007, Foreign National Security Controls at DoD Research Laboratories, October 27, 2000

Procedures at the Army Research Laboratory and the Air Force Research Laboratory-Munitions provided reasonable assurance that release of controlled unclassified and classified information to foreign nationals was in accordance with visit authorizations or certifications. However, the Defense Advanced Research Projects Agency and the Naval Research Laboratory controls over the dissemination of foreign disclosure instructions needed improvement. Specifically, for 208 of 270 official visits reviewed, the Defense Advanced Research Projects Agency and the Naval Research Laboratory did not disseminate foreign disclosure instructions to the program managers hosting foreign nationals. As a result, program managers were hosting foreign nations on official visits unaware of national security foreign disclosure restraints and may have inadvertently released unauthorized technical information to other countries. The Military Department laboratories' approval processes for visits by foreign nationals were adequate. However, the Defense Advanced Research Projects Agency security controls over the approval process for foreign national visitors were weak. Specifically, controls for granting building access for foreign national visitors representing U.S. entities required improvement. Also,

the Defense Advanced Research Projects Agency database contained inconsistent and inaccurate data. As a result, controls over the disclosure of controlled unclassified information to foreign nationals were not effective and U.S. personnel may have inadvertently disclosed controlled unclassified information to other countries, including countries of concern, without authorization.

FINANCIAL MANAGEMENT

D-2001-071, Navy Financial Reporting of Government-owned Materials Held by Commercial Shipyard Contractors, March 2, 2001

The Navy reported the value of Government-owned materials held by contractors using the Contract Property Management System database, which did not provide complete or accurate financial data that met the requirements of Federal accounting standards. Furthermore, the Navy overstated the value of $4.3 billion of Government-owned materials reviewed at five commercial shipyards by at least $1.4 billion for FY 1999. As a result, the Navy disclaimed the appropriateness of the balance on its financial statements for FY 1999. For FY 2000, the Navy is not reporting any values for Government-owned materials held by contractors on its financial statements. Until corrected, the Navy will continue to report incomplete and inaccurate financial data in FY 2001 and beyond.

D-2001-070, Internal Controls and Compliance With Laws and Regulations for the DoD Agency-Wide Financial Statements for FY 2000, February 28, 2001

The DoD could not provide sufficient or reliable information for us to verify amounts on the FY 2000 DoD Agency-Wide Financial Statements. We identified deficiencies in internal controls and accounting systems related to General Property, Plant, and Equipment; Inventory; Environmental Liabilities; Military Retirement Health Benefits Liability; and material lines within the Statement of Budgetary Resources. The DoD processed at least $4.5 trillion of department-level accounting entries to the DoD Components financial data used to prepare departmental reports and the DoD Agency-Wide financial statements for FY 2000. Also, $1.2 trillion in department-level accounting entries to financial data, used to prepare DoD Component financial statements, were unsupported because of documentation problems or improper because the entries were illogical or did not follow generally accepted accounting principles.

D-2001-042, Accounting and Disclosing Intragovernmental Transactions on the DoD Agency-Wide Financial Statements, January 31, 2001

Since FY 1996, DoD made little progress in accounting for and disclosing amounts of eliminating entries. Similarly, the Department has been slow to initiate improvements that are needed to ensure that all of the intragovernmental transactions were captured and the amounts were accurate. In response to prior audit reports, DoD indicated that it could not perform the critical checks because many of the accounting systems did not capture all the data necessary to reconcile with partners or to accurately identify elimination transactions and balances.

The FY 1999 DoD Agency-wide financial statements reflected $229.4 billion in intragovernmental transactions between buyers and sellers that were not reliable and were not adequately supported. The DoD reported $236.7 billion in eliminating entries that were not reconciled with intragovernmental accounts and buyer and seller transactions. The Defense Finance and Accounting Service made $298.8 billion (absolute value) in accounting entries to intragovernmental and public accounts that were not adequately reconciled. In addition, the elimination of intra-agency transactions on the Statement of Net Cost were made to the total program cost and revenue lines and not by the specific programs that made up the totals. As a result, the DoD Agency-wide financial statements continue to contain material misstatements, the amounts reported for intragovernmental line items are unreliable, and unless corrected, will continue to contain material misstatements for FY 2000 and beyond.

D-2001-024, Performance Measures for Disbursing Stations, December 23, 2000

The Defense Finance and Accounting Service (DFAS) lacked a plan to measure and improve the performance of disbursing stations in reconciling differences in deposits, interagency transfers, and checks issued. The DFAS did not measure the performance of:

- 353 (90.1 percent) of the 392 disbursing stations with deposit activity,
- 67 (64.4 percent) of the 104 disbursing stations with interagency transfer activity, and
- all 500 disbursing stations that issue checks.

As a result, DFAS could not identify disbursing stations with significant unreconciled differences. The disbursing stations

with the 10 largest average differences in deposits, interagency transfers, and checks issued accounted for $3.5 billion (58.3 percent) of the $6 billion average difference (absolute value) reported on the September 30, 1999, and April 30, 2000, Statements of Differences and Comparison Reports. Reconciliation of those disbursing stations' differences would significantly reduce the total DoD differences in deposits, interagency transfers, and checks issued and improve the accuracy and auditability of the DoD Fund Balance With Treasury account.

ACQUISITION

D-2001-066, Acquisition of the Advanced Tank Armament System (ATAS), February 28, 2001

The Army did not establish a viable acquisition strategy to develop and acquire the ATAS beyond the program definition and risk reduction phase. Instead, the milestone decision authority considered the ATAS to be a program element for funding technology demonstrations, but did not appropriately manage and fund ATAS as a technology demonstration. As a result, the Army obligated about $85.8 million in research, development, test, and evaluation funds through FY 2000 and planned to obligate another $62.9 million from FY 2001 through FY 2007 for a program that the Army was not intending to fund for the engineering and manufacturing development phase or the production phase of the acquisition process.

D-2001-061, Waivers of Requirement for Contractors to Provide Cost or Pricing Data, February 28, 2001

Contracting officials properly justified, and used in appropriate circumstances, waivers of the legal requirement to obtain cost or pricing data in an estimated 189 of the reviewed contract actions, valued at $1.0 billion, where waivers were used. Contracting officers also ensured fair and reasonable prices for those 189 contract actions. The procedures that DoD contracting organizations used to process the waivers and to determine fair and reasonable prices were effective and not burdensome.

The information on cost or pricing data in the Defense Contract Action Data System was very inaccurate and misleading. We estimated that 4,264 actions (92.9 percent), valued at $789 million, of 4,590 contract actions were miscoded. The significant errors grossly inflated the reported number of

contract actions in which the requirement for contractors to provide cost or pricing data had been waived.

D-2001-036, Acquisition of the Combat Survivor Evader Locator, January 25, 2001

The Combat Survivor Evader Locator Program Management Office had planned for and managed the design and development of the system well, despite funding shortfalls. The Air Force had been funding the system through internal Air Force reprogramming below the threshold that required congressional notification. During the audit, we had concerns regarding how the Program Management Office would fund additional interoperability and security requirements and associated technological challenges. Although the Program Management Office had requested the research, development, test and evaluation funds needed to address those requirements and challenges, the funds were not included in the Air Force FY 2002 Program Objective Memorandum. We also were concerned that the Air Force plan to incrementally purchase its hand-held radio requirements through FY 2038 would not take advantage of economic order quantities and, more importantly, would not satisfy a critical mission need in a reasonable timeframe. Those concerns have been addressed by revised programming guidance. If fully funded by Congress, this program can meet its objectives.

D-2001-032, Use of Exist Criteria for Major Defense Systems, January 10, 2001

For seven of the nine programs reviewed, milestone decision authorities did not ensure that program managers proposed program-specific exit criteria for use at the future milestone decision point(s). As a result, the milestone decision authorities were limited in their ability to use exit criteria as a management tool to determine whether programs under their review and oversight should progress within an acquisition phase or continue into the next acquisition phase at milestone decision points.

Program Managers for three of the five major Defense acquisition programs reviewed did not report their status toward attaining exit criteria requirements in the quarterly Defense Acquisition Executive Summary. As a result, milestone decision authorities and Office of the Secretary of Defense action officers did not have adequate information for assessing each program's progress toward satisfying exit criteria requirements and for providing direction, when needed, between milestone decision points.

D-2001-012, Acquisition of the Armored Medical Evacuation Vehicle (AMEV), November 22, 2000

The Army did not have a viable acquisition strategy to acquire the AMEV at the completion of the engineering and manufacturing development phase of the acquisition process. The Army had obligated about $9.7 million in research, development, test and evaluation funds for the program from its inception in FY 1997 through FY 2000. Another $6.3 million was earmarked to complete the developmental effort in FY 2001 through FY 2003 for the program, but the Army did not intend to fund production.

SUPPLY MANAGEMENT

D-2001-054, Defense Logistics Agency Product Verification Program, February 21, 2001

Defense Logistics Agency product test center planning procedures were logical and in conformance with test objectives. Testing was conducted using contract specifications and objectives, appropriate test equipment was used, and suspected deficiencies were evaluated. However, the product test selections and the use of test results needed improvement. Random product test selections did not include all products available for testing at all depots. For nonrandom testing, the Product Verification Office did not fully consider management's quality priorities and initiatives in test planning. As a result, funds for product testing were not used in the most efficient manner and DoD lacked sufficient assurance that some critical products would perform as expected. For two of the three Defense Supply Centers, test failures were not consistently investigated and required actions on test failures were not always taken. Inconsistent adjudication and ratings of test results hindered the two Defense Supply Centers from resolving contractor issues for 36 percent of the 231 FY 1999 tests we reviewed, inflated quality ratings for as many as 54 contractors and allowed potentially nonconforming products to remain available for issue.

D-2001-035, Management of Potentially Inactive Items at the Defense Logistics Agency, January 24, 2001

Defense Logistics Agency (DLA) managers needed to purge more National Stock Number (NSN) items, for which there is not longer a demand, from the supply system. As a result of the audit, the Defense Supply Center Philadelphia developed a computer program

to expedite the review process and deleted 20,385 of the 26,434 NSNs that had been in a review status over 90 days at the Center. However, because there are 64,663 more NSNs that still require DLA item manager review, we believe that the number of potentially inactive NSNs that could be deleted is significantly greater. We calculated that DLA avoided a minimum of $17.2 million of costs by eliminating unnecessary cataloging and supply system files, and by reducing inventory for the 20,385 NSNs. The full extent of the monetary benefits will be quantifiable after management identifies and takes action to delete all inactive NSNs and disposes of obsolete, excess inventory.

D-2001-002, Defense Logistics Agency Customer Returns Improvement Initiative Program, October 12, 2000

The Defense Logistics Agency did not fully implement the Customer Returns Improvement Initiative Program. Therefore, some depots could not screen and suspend potentially nonconforming assets received through customer returns. The Defense Supply Centers did not regularly transmit listings of nonconforming assets to the depots that participated in the program, nor did they consistently provide all necessary information to distinctly identify the assets. As a result, as many as 28 percent of the Defense Logistics Agency's returned assets, comprised of over 176,000 individual supplies and spare parts that had been identified as potentially defective and returned to the depots, were not screened and could be reissued to customers without qualification. Conversely, the lack of detailed information on nonconforming assets forwarded to the depots may have resulted in some assets being unnecessarily suspended.

PEACETIME HEALTH CARE

D-2001-037, Collection and Reporting of Patient Safety Data Within the Military Health System, January 29, 2001

Significant effort to collect and report patient safety data is ongoing at the Military Treatment Facility level within the Military Health System. The proposed DoD patient safety reporting program has the potential to improve data consistency and provide a means for sharing the data and lessons learned throughout DoD. To effectively and efficiently implement the proposed patient safety reporting program, an implementation strategy is needed. Without an implementation strategy, the

proposed program's potential for improving health care through reduction of medical errors may not be maximized.

READINESS

D-2001-059, Armed Services Blood Program Readiness, February 23, 2001

The Armed Services Blood Program relies on frozen red blood cells for contingency purposes. Inventories were short and related data were inaccurate. The DoD relies on frozen blood up to 21 years old, but the Food and Drug Administration standard for non-military stocks is a 10 year shelf life. Various other testing, training and planning issues needed attention.

D-2001-045, Government Performance and Results Act Goals: Tank Miles, February 7, 2001

The DoD reported 681 tank miles for FY 1999 instead of the 567 M1 Abrams tank miles actually driven, on average, in installation-based training. Further, DoD did not fully identify, document, and report the reasons for the 29 percent shortfall in achieving the 800 tank miles goal and actions taken to improve the ability of DoD to achieve the goal. The existing measure established performance objectives for training-only tank units rather than for the training for the Army's combat arms teams. Further, limitations on the use of the "Tank Miles" measures to assess the Army's ground forces were not clearly explained in the Annual Report. As a result, the "Tank Miles" performance measure report to Congress provided incomplete information and was not useful.

D-2001-033, Government Performance and Results Act: Unfunded Depot Maintenance, January 12, 2001

The March 2000 DoD performance report was not based on the best available data and was not supportable. The presentation of this important readiness metric needs improvement to make the report more meaningful and useful to DoD and Congress.

HUMAN CAPITAL

D-2001-008, Resources of DoD Adjudication Facilities, October 30, 2000

The number of personnel security clearance cases requiring adjudication was rising at a rate faster than most central

adjudication facilities' ability to process adjudicative decisions in a timely manner, because the facilities' resource requirements had not been fully identified and budgeted. Without corrective action, obtaining a security clearance could become an increasingly lengthy process for DoD personnel and contractors and DoD may be subjected to a higher risk of compromise.